Department of Justice

STATEMENT

OF

JAMES J. BANKSTON
CHIEF INSPECTOR
UNITED STATES MARSHALS SERVICE

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES

CONCERNING

"INTERNET DATA BROKERS AND PRETEXTING:

WHO HAS ACCESS TO YOUR PRIVATE RECORDS?"

PRESENTED ON

JUNE 22, 2006

STATEMENT OF JAMES J. BANKSTON
CHIEF INSPECTOR
UNITED STATES MARSHALS SERVICE
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES
JUNE 22, 2006

Good afternoon, Chairman Whitfield, Ranking Member Stupak, and members of the Subcommittee. Thank you for the opportunity to address the Subcommittee on this important technology-related privacy issue. My name is James J. Bankston. I am a Chief Inspector for the United States Marshals Service (USMS or Marshals Service), Investigative Services Division. As such, I provide headquarters-based managerial direction and oversight for the Marshals Service's criminal investigative mission.

The USMS shares the Subcommittee's concern over the inappropriate, if not illegal, collection and reselling of personal information by unscrupulous data brokers. In an age when consumers must cope all too often with the loss or mismanagement of their personal telephone, banking, credit card, and federal benefit information, the Subcommittee is to be commended for exploring ways to ensure that consumers' private information remains private and secure.

These efforts should not overlook the value of those reputable companies that acquire information from public or open sources; have security policies in place that fully explain the methods of collection, sale, and dissemination; monitor their security systems for breaches; and do not engage in "pretexting." Such companies have proven to be one of many invaluable resources that law enforcement agencies rely upon when conducting criminal investigations.

My testimony addresses three issues: 1) the USMS' concerns about the unrestricted and unregulated use of data brokers who use pretexting or other nefarious means to obtain private

records; 2) the USMS' use of legitimate data banks and resellers of public and open-source consumer information as just one of many tools utilized during the Agency's hundreds of thousands of criminal investigations; and 3) the internal audit conducted by the USMS to identify those instances where its employees may have used the data brokers who are under investigation by this Subcommittee.

Data Brokers

Like Congress and many of the consumer groups that have taken an interest in the commercial use of "data brokers" who claim to have access to telephone subscriber, call, and cell site usage, the USMS also is concerned about the unauthorized collection, sale, and distribution of this type of information. Individually, every USMS employee, as well as their family members, has expectations of privacy that mirror those of every other member of the public who engages in private, lawful conduct. At the same time, each Deputy U.S. Marshal is entitled to protection from criminal retribution for the critical law enforcement duties we perform. The USMS is involved in virtually every federal law enforcement initiative. As an agency, we are charged with the primary responsibility for identifying and investigating threats and providing protection to thousands of federal judges, jurors, U.S. Attorneys, Assistant U.S. Attorneys, witnesses, and other persons designated by Congress or the Department of Justice. In addition to protecting the integrity of the federal justice system, the USMS operates the Witness Security Program, transports federal prisoners, and seizes property acquired by criminals through illegal activities. Further, USMS is the federal government's primary agency for conducting fugitive investigations. We arrest more than half of all federal fugitives.

Unregulated access to subscriber information, call detail records, and the dates and times

that individual cell sites are accessed would wreak havoc on our efforts and ability to assure the operational security of our protectees and their families, associates, and routines, as well as our other law enforcement responsibilities. Restrictions that protect privacy are reasonable and necessary, and abuses should be thoroughly investigated and eliminated.

USMS Investigations and the Use of Open-Source Information

The USMS is a significant consumer of lawfully-obtained public and open-source records. In order to fulfill our mandate to investigate and apprehend violent criminals wanted at the federal, state, and local levels, as well as to investigate threats against the federal judiciary, the timely acquisition, analysis, and reduction of voluminous open-source records into "actionable intelligence" has played, and continues to play, a significant role in our swift and unparalleled success in apprehending some of the nation's most notorious and dangerous fugitives.

The USMS, like other agencies, utilizes certain data banks and commercial sources of information under contractual agreements sanctioned by the Department of Justice. Such services are used only as needed and pursuant to a specific and legitimate law enforcement investigative inquiry. While federal law enforcement agencies like the USMS now have access to legitimately-collected information that was previously unavailable from a single-collection point, such access is absolutely essential to our ability to stay one step ahead of seasoned and resourceful criminals desperate to evade justice.

One of the USMS' primary criminal investigative missions involves locating and apprehending fugitives who are on the run from the law. Our fugitive mission has a singular purpose – to swiftly apprehend a known fugitive to answer for the charges. Fugitives from

justice have already experienced varying degrees of due process, from a grand jury indictment to a trial by peers to appellate review. Unlike law enforcement agencies that are responsible for investigating ***who*** committed a crime, the USMS does not seek to build a prosecutorial case against an individual. In nearly every case, we know exactly who is wanted; our goal is to end the investigation by fulfilling a court-ordered arrest warrant and bringing a wanted fugitive to justice.

A violent fugitive – the most common target of a USMS investigation – is a unique target among law enforcement investigations in that, at a minimum, an independent grand jury or a neutral and detached judge already has determined that probable cause exists to believe that a crime has been committed and that the named fugitive committed the crime. Many of the individuals whom the USMS investigates are post-conviction fugitives (such as parole violators, probation violators, or failure to surrender fugitives) who have pled guilty or have been found guilty by jury or judge. The USMS also is responsible for apprehending the most dangerous class of fugitive – the violent escapee who will do just about anything to avoid apprehension.

These investigations include not only the tens of thousands of federal fugitives that the USMS tracks and captures, but also the many more state, county, and local fugitives we investigate as part of our six regional fugitive task forces and more than 90 district-based multi-agency task forces. In fiscal year 2005, the USMS arrested more than 35,500 federal fugitive felons and cleared 38,500 federal felony warrants – more than all other federal law enforcement agencies combined. Together with our federal, state, and local partners, U.S. Marshals-led fugitive task forces arrested more than 44,000 state and local fugitives and cleared 51,200 state and local felony warrants. These results are unparalleled in law enforcement.

As of June 13, 2006, the USMS fugitive caseload consisted of 36,464 federal felony fugitives and 13,396 state felony fugitives. On any given day, USMS employees make hundreds of requests for information from a variety of sources. Many of those requests involve the use of data banks and open-source materials as a supplement to basic police investigative leg-work, and eventually aid in making an apprehension and taking a violent criminal off the streets. For example, in the last three months alone, criminal investigators and intelligence analysts assigned to the Criminal Information Branch of the Marshals Service's Great Lakes Regional Fugitive Task Force, based in Chicago, have used commercial databases and open-source data banks such as Lexis-Nexis/Accurint and ChoicePoint to obtain critical information that directly led to the arrests of the following violent fugitives:

- ***Dimitrie Thomas, Sean Everett, and Andre Jones,*** who were wanted in Cabell County, West Virginia. Thomas and Jones were wanted for narcotics violations, while Everett was wanted on federal weapons charges. Deputies seized two fully-loaded handguns, a revolver and a shotgun, while searching Thomas' residence after his arrest. All three were arrested in Detroit, Michigan.
- ***Roberto I. Lopez,*** who was wanted in Milwaukee, Wisconsin, for first-degree murder and armed robbery in a drug-related case. Marshals Service investigators determined that Lopez had fled to his native Dominican Republic, where he had been using a number of aliases to avoid detection. Lopez was arrested by local authorities with the assistance of the USMS Dominican Republic Foreign Field Office.

- ***Corey Moss,*** who was wanted in Waukesha County, Wisconsin, for sexual assault. He was arrested in Milwaukee by Deputies who found him hiding in a basement of his mother's home.

Open-source information also was critical to the success of the fugitive investigation of ***Timothy Berner***, who was wanted in Sterling Heights, Michigan, for the July 2004 murder of Police Officer Mark Sawyer. Berner had committed several bank robberies with a shotgun, and he specifically targeted Officer Sawyer so that he could steal his service revolver and continue his criminal ways. As Officer Sawyer sat in a shopping center parking lot writing routine police reports, Berner approached and fired a single shot, killing him. He then stole Officer Sawyer's handgun and fled the scene. For three weeks, Deputy U.S. Marshals and task force officers from a variety of districts tracked Berner to Jacksonville, Florida, where he was located at the residence of a female acquaintance who was unaware of his real identity and crimes. As investigators approached to arrest him, Berner committed suicide.

The cases I just cited are just four of tens of thousands of fugitive investigations that the Marshals Service undertakes each year. I could provide hundreds of similar examples where USMS criminal investigators and intelligence analysts have used these resources in fugitive investigations and made an arrest.

USMS Data Broker Queries

The Subcommittee has obtained a document signed by a Deputy U.S. Marshal requesting information from a company currently under the Committee's scrutiny. After thorough inquiry, we have ascertained that the Deputy's intent was to obtain subscriber information on a cell phone number as part of a fugitive investigation. Our survey of the 94 USMS districts, six regional fugitive task forces, five Regional Technical Operations Centers, and financial records has revealed only this isolated instance of use of the data brokers in question.

While no formal policy currently exists specifically addressing the use of data brokers of the type under investigation by this Subcommittee, USMS investigators and analysts are trained to keep their information collection within established legal boundaries. Defined legal boundaries of investigative endeavors are present through USMS policy pertaining to fugitive investigations and technical operations. Moreover, the Department of Justice has created a Privacy and Civil Liberties Board to ensure that Departmental programs and efforts adequately consider civil liberties and privacy. The Data Committee of the Privacy and Civil Liberties Board, on which USMS is represented, was established earlier this year to address issues related to information privacy within the Department. Its first task is to respond to recommendations in the April 2006 GAO report entitled "Personal Information Agency and Reseller Adherence to Key Privacy Principles." The Data Committee members are analyzing the Department's use of all information reseller data, including internet data brokers, and will evaluate potential Department-wide policy with regard to such use. Specifically, all members of the committee are currently assessing their agencies' use of information reseller data, including the Internet data brokers identified by the Subcommittee as employing pretexting and fraud to obtain information. While the inquiry is ongoing, to this point, there is no evidence of widespread use of such

services. The Data Committee meets on a monthly basis and expects to make recommendations to the Attorney General on this issue upon completion of its review.

Conclusion

The USMS has a legitimate need to investigate a wide variety of sources in order to obtain personal information that might lead to the ultimate apprehension of wanted fugitives. The need to acquire information quickly is critical to the success of our investigative efforts. Ultimately, the USMS needs information to locate and bring the wanted fugitive to justice. Today's fugitive is often a hardened criminal who has had the benefit of a few years in prison to sharpen and refine his skills, and is keenly aware of both our capabilities and our weaknesses.

Just as the electronic age has brought with it great advances in the speed and accuracy with which information is collected, stored, and retrieved, so too has it brought increased risk to law enforcement, particularly agents operating undercover: 1) the virtual contemporaneous disclosure of investigative techniques; 2) the detailed disclosure of precisely what records are maintained and, therefore, available to law enforcement; 3) the disclosure of investigative technology, capability, and limitations; 4) the ability to communicate anywhere and anonymously behind "ported" numbers and prepaid phones with no listed subscribers; 5) off-shore calling cards obtained either through convenience stores or the Internet; and 6) point-to-point encrypted packet-data communications.

Over time, we have had to refocus our investigative efforts and techniques to address this newly emerging class of experienced criminal. Access to legitimate resources must be retained in order to allow law enforcement to stay one step ahead of the individuals who are all too willing to circumvent the law. Similarly those would circumvent established legal or ethical principles to obtain private information must be prevented from doing so.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions you or other members of the Subcommittee may have.